SPYWOLF

Security Audit Report

Completed on

April 26, 2023

OVERVIEW

This audit has been prepared for **ShibAnon** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

ShibAnon

PROJECT DESCRIPTION

According to their litepaper:

Shibanon was created to become the first mixer on the Shibarium chain. Staying true to the core essence of decentralization, Shibanon will provide ultimate privacy to your transactions while utilizing their platform. The purpose of this unique mixer dApp executing this function, is to ensure investors on the Shibarium chain maintain their privacy with every transaction.

Release Date: Main token launches on May 1, 2023

Category: Crypto mixer

CONTRACT INFO

Token Name	Symbol
ShibaStaking	N/A

Contract Address
0x85C0a331F3Ebf3E5586F759DF678a36Fc3200Fc9

Network	Language
Polygon **TESTNET**	Solidity

Deployment Date	Verified?
Apr 24, 2023	Yes

Total Supply	Status
N/A	Launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	N/A
External calls	N/A
Internal calls	N/A
Transactions count	N/A
Uniq Callers	N/A
Days contract called	N/A
Last transaction time	N/A
Created	N/A
Create TX	N/A
Creator	N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can change token contract required for staking.
Owner can withdraw any tokens from the contract.

```
function setTokenContract(address _newContract) public onlyOwner {
    require(_newContract != address(0), "Please provide a valid address");
    TokenContract = _newContract;
}

function withdrawFunds(uint256 _amount) external onlyOwner nonReentrant {
    // transfer fund
    IERC20(TokenContract).safeTransfer(msg.sender, _amount);
}
```

FOUND THREATS

⚠ Medium Risk

Owner can change deposit fees up to 99.9%.
This is the amount that will be deducted from each user deposit.

```
function setDevFee(uint16 _devFee) public onlyOwner {
    require(_devFee < 10000, "Dev Fee rate shouldn't be greater than 10000(100%).");
    developerTax = _devFee;
    emit DevFeeChanged(_devFee, block.timestamp);
}

function deposit(uint _amount) external {
    require(_amount > 0, "You need to deposit more than zero");
    IERC20(TokenContract).safeTransferFrom(msg.sender, address(this), _amount);
    uint256 depositFee = (_amount * developerTax).div(percentRate);
..............
}
```

Informational

Owner can set the period required to claim rewards without limitation.
This is the time that users must wait before able to claim rewards after their deposit.

```
function setRewardPeriod(uint256 _rewardPeriod) public onlyOwner {
    rewardPeriod = _rewardPeriod;
}

function claimReward() external nonReentrant {
.................
    uint256 RoiTime = block.timestamp - depositInfo[msg.sender].depositAt;
    require(RoiTime > rewardPeriod, "You can claim after lock period");
.................
}
```

Owner can change the NFT cotnract required for NFT APR yield.

```
function setNFTContract(address _newContract) public onlyOwner {
    require(_newContract != address(0), "Please provide a valid address");
    nftContract = NFTContract(_newContract);
}
```

Owner can change NFT yield and regular yield percents up to 99.9% of user's deposit.

```
function setApr(uint16 _apr0, uint16 _apr1) public onlyOwner {
    require(_apr0 < 10000 && _apr1 < 10000, "APR shouldn't be greater than 10000(100%).");
    apr0 = _apr0;
    apr1 = _apr1;
    emit AprChanged(apr0, block.timestamp);
}
```

Informational

There is 10% early withdraw fee applied if users withdraws their funds before the rewardPeriod is expired.
Current rewardPeriod is 3 days.

```
uint256 public rewardPeriod = 3 days;
uint16 public withdrawTax = 1000;
uint16 public constant percentRate = 10000;

function withdrawCapital(uint _amount) external nonReentrant {
.................
    uint withdrawFee = (_amount * withdrawTax).div(percentRate);
    uint256 RoiTime = block.timestamp - depositInfo[msg.sender].depositAt;
    if (RoiTime > rewardPeriod) {
        withdrawFee = 0;
    }
.................
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

ShibAnon Staking

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.